A Quantitative Study of Firewall Configuration Errors

Avishai Wool

IEEE Computer, June 2004

18/10/2004

Presented by Joe Ling

Summary of the Article

- This article gives a constructive analysis result of “real” corporate firewall configuration errors behind the scenes.

Appreciative Comment

- The collected data is being analysed in a constructive way with useful result that can give us an idea of the real firewall configuration.
  - The twelve possible configuration errors have successfully pinpoint the errors in the sample rule-sets.
  - The rule-set complexity makes a good prediction of the number of configuration errors.

The Rule-Set Complexity

RC = Rules + Objects + Interfaces(Interfaces – 1)/2

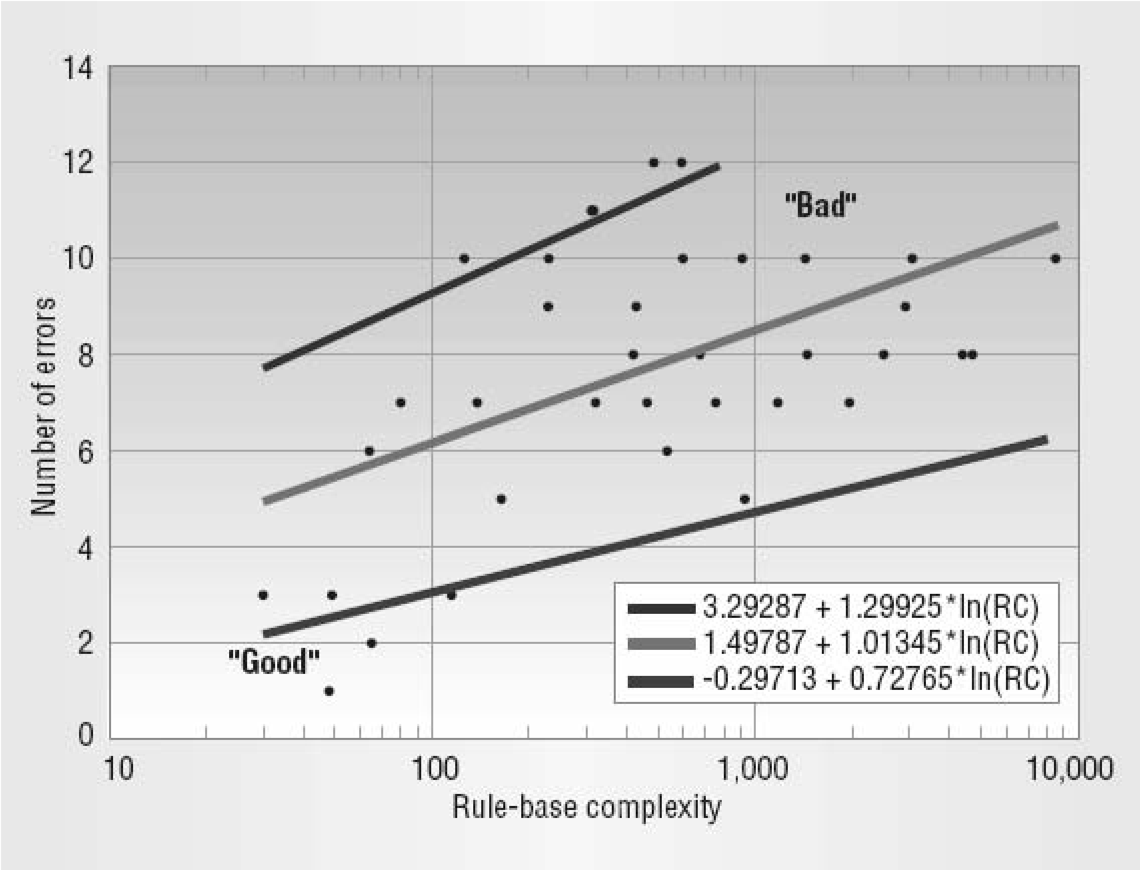

Figure 4. Number of errors as a function of rule-set complexity

- A linear relationship is between RC and number of errors.
- Most corporate firewalls are having poorly written rule sets.
- Only small numbers of firewalls are being well configured.
- Small and simple rule set is no guarantee of a good configuration.

18/10/2004

Critical Comment (1)

- The accuracy and representative of the result is questionable due to the small, self-selected and not up-to-date sample.
  - Only 37 firewall rule-sets sample out of hundred of thousands are being examined.
  - The sample is come from the organizations that willing to pay for an audit of their firewall rule set by an external company. It may bias the sample toward badly configured firewalls.
  - Data are collected between 2000 and 2001 which is three year ago.

Critical Comment (2)

- The conclusion “for well-configured firewalls, small is beautiful” is arguable.
  - The inaccurate sample data may gives incorrect result.
  - Our network is growing in tremendous speed that results in a much more complex network compare with three years ago.
  - A complex network simply cannot be managed by a small and simple rule-set.

Question

- Conclusion from the author, “For well-configured firewalls, small is beautiful”.
- Does it apply to nowadays network?

Thank you